APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,444	01/12/2004	Balaji Vembu	042390.P18507	2132

45209   7590   06/23/2008
INTEL/BLAKELY
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER
PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>06 May 2008</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-4,6-12 and 14-21</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-4, 6-12, 14-21</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/6/2008 has been entered.

Response to Arguments

Applicant's arguments filed 5/6/2008 have been fully considered but they are not persuasive. The Applicant makes one argument that the TPM being separate from the application program and graphics device distinguishes from cited prior arts.

Hillier discloses the 3rd Party Processor being separate from the orig. processor or recipient processor see Fig. 1.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

Claims 1-5,7-13, 16, are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121 to

Lyson et al.(hereinafter Lyson) further in view of US Patent 6256733 to Thakkar et al.(hereinafter Thakkar) and further in view US Patent 2004/0151319 to Proudler.

Regarding Claim 1, 10, Hillier discloses the first entity(originator processor) having associated with a key(KS1) , second entity(recipient processor) associated with a key(2ndEPuK) and third entity(third party processor) associated with a key(3rdEPuk) being separate from first entity and second entity see Fig. 1 & Col 5 Ln 41- Col 6 Ln 13; decrypting of keys(KS2, KS, KS1) using third party's private keys see Col 6 Ln 3-13 & Col 7 Ln 5-20. But fails to explicitly disclose the encrypting the first key by the second key and another entity obtaining this key and further decrypting the first key encrypted by second key. However, Lyson discloses the re-encrypting the captured data and further of a requesting entity decrypting the encrypted key to obtain key see Fig. 3 item 70, 72, 74 & Col 5 Ln 40-51 & Col 6 Ln 19-23. It would be obvious to one having ordinary skill in the art at the time of the invention to include the re-encrypting of captured data and decrypting to obtain key in the invention of Hillier in order to have a reduced number of keys as taught in Lyson see Col 2 Ln 39-44. Neither Hillier nor Lyson explicitly disclose the encrypting of keys using the public key of an entity. However, Thakkar discloses the encrypting of keys using the public key see Col 1 Ln 37-53. It would be obvious to one having ordinary skill in the art at the time of the invention to include the use of encrypting key using public keys in the invention of Hillier in order to provide for signature verification using publicly available data as taught in Thakkar see Col 1 Ln 36-46. Neither Hillier nor Lyson nor Thakkar disclose the TPM.

However, Proudler discloses the TPM as being an entity that is used for encrypting

using key see Fig. 3 item 10. It would be obvious to one having ordinary skill in the art at

the time of the invention to include TPM in the invention of Hillier in order to perform the

encrypting operation in a TCPA specified chip as taught in Proudler see Par. 0003.

Regarding Claim 2, 16, Hillier discloses direct communication between originator and

recipient after connection see Col 4 Ln 23-27.

Regarding Claim 3-4, 11-12, Hillier discloses the processor, which includes an graphics

device and application program see Fig. 1 item 12, 14.

Regarding Claim 5, 13, Hillier discloses the trust third party see Col 2 Ln 16-20.

Claims 6, 14-15, 17, 20, are rejected under 35 U.S.C. 103(a) as being unpatentable

over US Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121

to Lyson et al.(hereinafter Lyson) further in view of US Patent 2003/0194093 to Evans

et al.(hereinafter Evans).

Regarding Claim 6, 15, Hillier nor Lyson explicitly disclose the pseudo-randomly

generated keys. However, Evans discloses the pseudo-randomly generated keys see

Par. 0067. It would be obvious to one having ordinary skill in the art at the time of the

invention to include the pseudo-randomly generated keys in the invention of Hillier in

order to have key that is never revealed as taught in Evans see Par. 0067 & Par. 0068.

Regarding Claim 14, 17, 20, Hillier nor Lyson explicitly disclose registers for storing

keys or input/output pin dedicated to use by first entity. However, Evans discloses the

registers for storing keys see Par. 0028 and input/output pin dedicated to use by first

entity see Par. 0031 & Par. 0029. It would be obvious to one having ordinary skill in the

art at the time of the invention to include registers in the invention of Hiller in order to

have a unit for storing keys as taught in Evans see Par. 0029.

Claims 18-19, 21, are rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent 7142676 to Hillier et al.(hereinafter Hillier) in view of US Patent 6336121 to

Lyson et al.(hereinafter Lyson) further in view of US Patent 6256733 to Thakkar et

al.(hereinafter Thakkar) further in view of US Patent 2003/0194093 to Evans et

al.(hereinafter Evans) and further in view of US Patent 2004/0151319 to Proudler.

Regarding Claim 18, Hillier discloses the first entity(originator processor) having

associated with a key(KS1) , second entity(recipient processor) associated with a

key(2ndEPuK) and third entity(third party processor) associated with a key(3rdEPuk)

being separate from first and second entity see Fig. 1 & Col 5 Ln 41- Col 6 Ln 13;

decrypting of keys(KS2, KS, KS1) using third party's private keys see Col 6 Ln 3-13 &

Col 7 Ln 5-20. But fails to explicitly disclose the encrypting the first key by the second

key and another entity obtaining this key and further decrypting the first key encrypted

by second key. However, Lyson discloses the re-encrypting the captured data and

further of a requesting entity decrypting the encrypted key to obtain key see Fig. 3 item

70, 72, 74 & Col 5 Ln 40-51 & Col 6 Ln 19-23. It would be obvious to one having

ordinary skill in the art at the time of the invention to include the re-encrypting of

captured data and decrypting to obtain key in the invention of Hillier in order to have a

reduced number of keys as taught in Lyson see Col 2 Ln 39-44. Neither Hillier nor

Lyson explicitly disclose the encrypting of keys using the public key of an entity.

However, Thakkar discloses the encrypting of keys using the public key see Col 1 Ln

37-53. It would be obvious to one having ordinary skill in the art at the time of the

invention to include the use of encrypting key using public keys in the invention of Hillier

in order to provide for signature verification using publicly available data as taught in

Thakkar see Col 1 Ln 36-46. Further yet, Hillier nor Lyson nor Thakkar explicitly

disclose the pseudo-randomly generated keys. However, Evans discloses the pseudo-

randomly generated keys see Par. 0067. It would be obvious to one having ordinary skill

in the art at the time of the invention to include the pseudo-randomly generated keys in

the invention of Hillier in order to have key that is never revealed as taught in Evans see

Par. 0067 & Par. 0068. Further, Hillier nor Lyson explicitly disclose registers for storing

keys or input/output pin dedicated to use by first entity. However, Evans discloses the

registers for storing keys see Par. 0028 and input/output pin dedicated to use by first

entity see Par. 0031 & Par. 0029. It would be obvious to one having ordinary skill in the

art at the time of the invention to include registers in the invention of Hiller in order to

have a unit for storing keys as taught in Evans see Par. 0029. Neither Hillier nor Lyson

nor Thakkar disclose the TPM. However, Proudler discloses the TPM as being an entity

that is used for encrypting using key see Fig. 3 item 10. It would be obvious to one

having ordinary skill in the art at the time of the invention to include TPM in the invention

of Hillier in order to perform the encrypting operation in a TCPA specified chip as taught

in Proudler see Par. 0003.

Regarding Claim 19, Hillier discloses the signal the start of key exchange see Fig. 3a

item 42.

Regarding Claim 21, Hillier discloses the decrypting the encrypted content see Fig. 4

item 55.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Venkat Perungavoor whose telephone number is

(571)272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to

reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto

Barron can be reached on 571-272-3799. The fax phone number for the organization

where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. P./
Examiner, Art Unit 2132
June 16, 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132